




DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT SYSTEM AUDIT CONTROLS	POLICY NO. 558.01	EFFECTIVE DATE 04/20/2005	PAGE 1 of 2
APPROVED BY:  Director	SUPERSEDES 500.44 04/20/2005	ORIGINAL ISSUE DATE	DISTRIBUTION LEVEL(S) 1

PURPOSE

- 1.1 To ensure audit control mechanisms that record and examine system activity are in place for all departmental electronic information systems.

POLICY

- 2.1 The Department of Mental Health (DMH) must ensure that data systems containing Protected Health Information (PHI) and other confidential information utilize a mechanism to log and store system activity in accordance with the recommended safeguards specified in the DMH Master Security Management Report, DMH Policy No. 550.01, Security Management Process: DMH Risk Management.
- 2.2 DMH must develop an Audit Control and Review Plan that describes the systems and applications to be logged, activities to be audited, responsibilities of Workforce Members involved in the implementation of the Plan (including separation of duties), frequency of audits, and the audit reporting and review process. The Plan must be reviewed and approved by the Departmental Information Security Officer (DISO) or designee.
- 2.3 DMH must protect the confidentiality, availability, and integrity of audit trails and internal audit reports.
- 2.4 DMH must ensure that audit trails are backed up and that the backups are verified and tested to assure complete restoration capability.

DEFINITIONS

- 3.1 Audit Trail: Detailed logs of who did what and when and also if there are any attempted security violations. These logs, maintained by the data security system, provide



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
SYSTEM AUDIT CONTROLS	558.01	04/20/2005	2 of 2

information that allows the system auditor to determine who initiated the transaction, the time of the day and date of entry, the type of entry, what fields of information were affected, and the terminal used.

- 3.2 Workforce Member: Employees, volunteers, trainees, and other persons whose conduct in the performance of work for the Department, its offices, programs or facilities, is under the direct control of the Department, office, program, or facility, regardless of whether they are paid by the Department.

PROCEDURE

- 4.1 Follow the procedures detailed in Attachment I.

AUTHORITY

MANDATED BY 45 Code of Federal Regulations (CFR) Part 164, §164.132(b)
Board of Supervisors Policies: 6.107, Information Technology Risk Assessment; and
6.108, Auditing and Compliance

CROSS REFERENCES

DMH Policies: 550.01, Security Management Process: DMH Risk Management; and
550.03, Information Technology Contingency Plan

ATTACHMENT

Attachment I DMH Systems Audit Controls Procedure

REVIEW DATE

This policy shall be reviewed on or before January 2010.